(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 982 958 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
10.01.2001 Bulletin 2001/02

(51) Int Cl.[7]: **H04Q 7/32**

(43) Date of publication A2:
01.03.2000 Bulletin 2000/09

(21) Application number: **99306466.6**

(22) Date of filing: **17.08.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **28.08.1998 US 141582**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

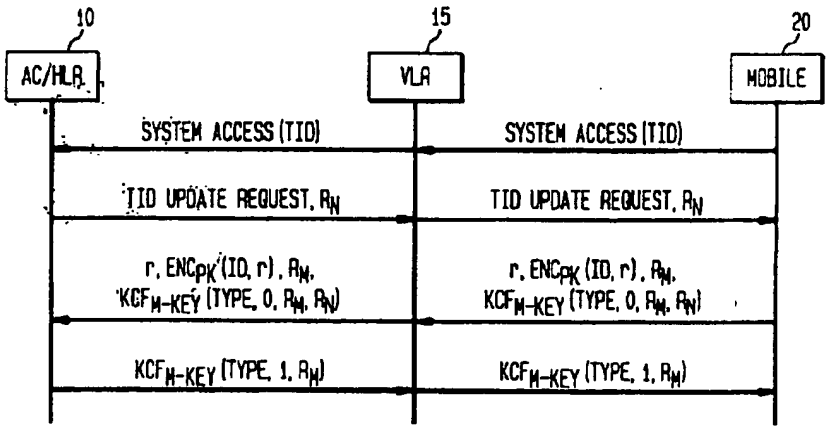
(72) Inventor: **Patel, Sarvar**
Montville, NJ 07045 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) Method for protecting mobile anonymity

(57) In the method for protecting mobile anonymity, the network sends a temporary mobile identifier (TID) update request to the mobile along with a challenge. In response, the mobile encrypts its permanent ID through public key encryption using the public key of the network, and sends the encryption result to the network. Also, the mobile generates a second challenge, and a first challenge response. The first challenge response is generated by performing a keyed cryptographic function (KCF) on the first and second challenges using a key. The mobile sends the second challenge and the first challenge response to the network with the encrypted permanent ID. After decrypting the permanent ID, the network accesses the key associated with mobile using the permanent ID. Next, using the key, the network authenticates the mobile using the second challenge and the first challenge response. If authenticated, the network calculated a TID for the mobile using the first and second challenges. The network further generates and sends a second challenge response to the mobile. If the mobile authenticates the network based on the second challenge response, then the mobile calculates the TID in the same manner as did the network.

FIG. 2



EP 0 982 958 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 30 6466

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	PARK CH -S: "ON CERTIFICATE-BASED SECURITY PROTOCOLS FOR WIRELESS MOBILE COMMUNICATION SYSTEMS" September 1997 (1997-09) , IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS,IEEE INC. NEW YORK,US, VOL. 11, NR. 5, PAGE(S) 50-55 XP000699941 ISSN: 0890-8044 * page 50, line 10 - page 54, line 45 *	1,3-17	H04Q7/32
Y	CAMPANINI G ET AL: "PRIVACY, SECURITY AND USER IDENTIFICATION IN NEW GENERATION RADIOMOLBILE SYSTEMS" 30 June 1987 (1987-06-30) , INTERNATIONAL CONFERENCE ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS,XX,XX, PAGE(S) 152-164 XP002040784 * page 152, line 1 - page 161, line 15 * * figure 1 *	1,3-17	
A	WO 98 26538 A (NOKIA TELECOMMUNICATIONS OY ;JUOPPERI JARI (FI)) 18 June 1998 (1998-06-18) * page 6, line 25 - page 13, line 16 * * figures *	1-18	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q
A	AREND VAN DER P C J: "SECURITY ASPECTS AND THE IMPLEMENTATION IN THE GSM-SYSTEM" 12 October 1988 (1988-10-12) , PROCEEDINGS OF DIGITAL CELLULAR RADIO CONFERENCE,XX,XX, PAGE(S) 4A-1-4A-07 XP000618482 * the whole document *	1-18	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	16 November 2000	Psatha, H

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 30 6466

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-11-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9826538 A	18-06-1998	FI 964926 A	11-06-1998
		AU 5190898 A	03-07-1998
		EP 0963636 A	15-12-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82